

# Threat Intelligence & The hateful eight: Common TTPs of the Modern Ransomware Groups

Nikita Nazarov,  
Head of Threat Exploration



---

## О чём будем говорить:

2

### Первая часть:

- Cyber Kill Chain как начало точки отсчёта современного TI;
- F2T2EA - FIND FIX TRACK TARGET ENGAGE ASSESS;
- Intelligence-Driven Defense;
- Рождение MITRE ATT&CK®;
- Пирамида боли Дэвида Бианко;

### Вторая часть:

- The hateful eight: Common TTPs of the Modern Ransomware Groups

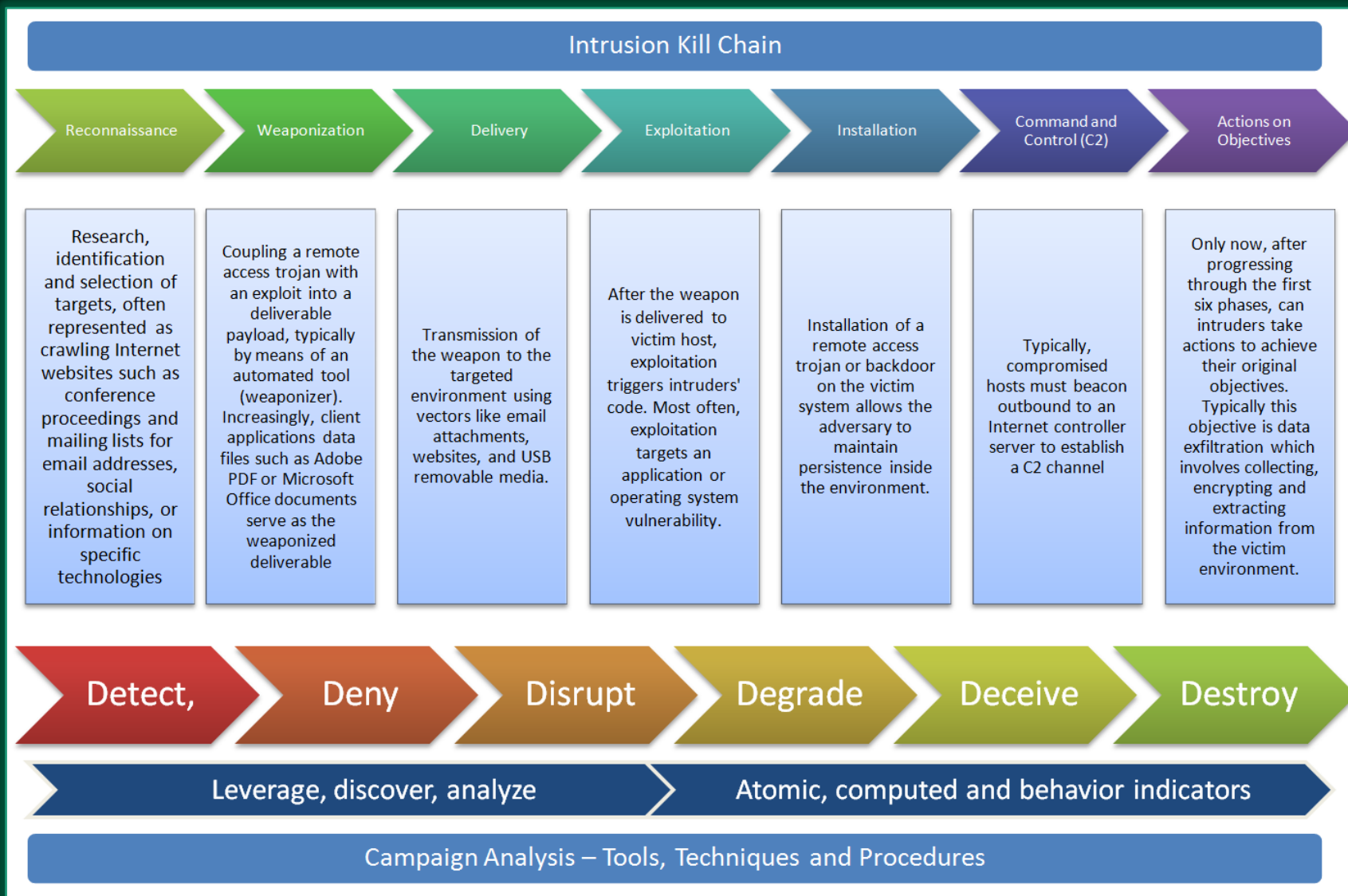
“

“Если знаешь противника и знаешь себя, сражайся хоть сто раз, опасности не будет; если знаешь себя, а его не знаешь, один раз победишь, другой раз потерпишь поражение; если не знаешь ни себя, ни его, каждый раз, когда будешь сражаться, будешь терпеть поражение.”



# Cyber Kill Chain

4



1996 F2T2EA

2011 Cyber Kill Chain

2012 Intelligence - Driven Defense

2013 - ATT&CK Matrix



Figure 1-1. F2T2EA

The Find, Fix, Track Target, Engage, Assess (F2T2EA) methodology seen in Figure 1-1 mechanizes the operational level "kill chain" during the execution process. Theater and national assets/resources detect objectives of potential significance (find). These systems identify and determine the location of a target (fix). From this location, tracking systems acquire and monitor the object (track). Dynamic decision-making then directs resources (target), and applies capabilities (engage) in a timely and decisive manner. To assure the desired effect, an assessment (assess) occurs during or after engagement to determine whether the target should be reattacked. These sequential steps describe a critical path that must occur for each dynamic event.

1996 F2T2EA

2011 Cyber Kill Chain

2012 Intelligence - Driven  
Defense

2013 - ATT&amp;CK Matrix

TABLE I. KEY INDICATORS OF KILL CHAINS

Phase	Indicators
Find	detection range(km), transmit power(kW), endurance(h), working frequency(MHz), pulse width( $\mu$ s), pulse repetition rate(kHz), antenna length(m), radome thickness(m), azimuth beam width( $^{\circ}$ ), elevation beam width( $^{\circ}$ ), antenna side lobe (dB)
Fix	transmit power(kW), received frequency(MHz), dynamic range(dB), sensitivity(dBv), output power(kW), MTBF(h), peak power(w), recognition range (km)
Track	target tracking capacity, angular accuracy( $^{\circ}$ ), velocity measurement range (kn) , clutter improvement factor(dB), operating range(km), endurance(h), MTBF(h)
Target	navigation capability, target processing capacity, azimuth( $^{\circ}$ ), data transfer rate(kbps), working frequency(MHz), operating range(km)
Engage	tactical range(km), service ceiling(m), maximum suspension weight(kg), maximum level flight speed(km/h), hitting probability(%),maximum attack range(km), maximum missile speed(km/h)
Assess	endurance(h), transmit frequency(MHz), received frequency(MHz), dynamic range(dB), sensitivity(dBv) , operating range(km) , MTBF(h)

## Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric M. Hutchins\*, Michael J. Cloppert†, Rohan M. Amin, Ph.D.‡

Lockheed Martin Corporation

### Abstract

Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insufficient for certain actors. A new class of threats, appropriately dubbed the “Advanced Persistent Threat” (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the adversary’s likelihood of success with each subsequent intrusion attempt. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND). Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness. The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component of risk, too.

1996 F2T2EA

2011 Cyber Kill Chain

2012 Intelligence - Driven  
Defense

2013 - ATT&CK Matrix

# Intelligence-Driven Defense - Courses of Action

7

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

1996 F2T2EA

2011 Cyber Kill Chain

2012 Intelligence - Driven  
Defense

2013 - ATT&CK Matrix

“Если хочешь идти быстро — иди один, если хочешь идти далеко — идите вместе.”

---

Африканская пословица



layout: side ▾    show sub-techniques    hide sub-techniques


Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (5)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (2)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (2)	Exfiltration Over C2 Channel	Data Manipulation (2)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Create or Modify System Process (4)	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Defacement (2)	Disk Wipe (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Domain Policy Modification (2)	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (2)	Scheduled Task/Job (6)	Create Account (2)	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	Container and Resource Discovery	Data from Information Repositories (2)	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Technical Databases (5)		Trusted Relationship	Software Deployment Tools	Create or Modify System Process (4)	Event Triggered Execution (15)	Event Triggered Execution (15)	Modify Authentication Process (4)	File and Directory Permissions Modification (2)	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Open Websites/Domains (2)		Valid Accounts (4)	System Services (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	OS Credential Dumping (6)	Network Sniffing	Use Alternate Authentication Material (4)	Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
Search Victim-Owned Websites			User Execution (3)	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Service Scanning		Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	System Shutdown/Reboot
			Windows Management Instrumentation	Implant Internal Image	Process Injection (11)	Indicator Removal on Host (6)	Steal or Forge Kerberos Tickets (4)	Network Share Discovery		Proxy (4)	Remote Access Software		
				Modify Authentication Process (4)	Scheduled Task/Job (6)	Indirect Command Execution	Steal Web Session Cookie	Password Policy Discovery		Data Staged (2)	Traffic Signaling (1)		
				Office Application Startup (6)	Valid Accounts (4)	Masquerading (7)	Two-Factor Authentication Interception	Peripheral Device Discovery		Email Collection (2)	Web Service (2)		
				Pre-OS Boot (5)		Modify Cloud Compute Infrastructure (4)	Unsecured Credentials (7)	Process Discovery		Input Capture (4)			
				Scheduled Task/Job (6)		Modify Registry		Query Registry		Screen Capture			
				Server Software Component (4)		Modify System Image (2)		Remote System Discovery		Video Capture			
				Traffic Signaling (1)		Network Boundary Bridging (1)		Software Discovery (1)					
				Valid Accounts (4)		Obfuscated Files or Information (6)		System Information Discovery					
						Pre-OS Boot (5)		System Location Discovery (1)					
						Process Injection (11)		System Network Configuration Discovery (1)					
						Reflective Code Loading		System Network Connections Discovery					
						Rogue Domain							

## 2013 - ATT&CK Matrix

# MITRE ATT&CK

10

Reconnaissance 10 techniques		Resource Development 7 techniques		Initial Access 9 techniques		Execution 12 techniques		Persistence 13 techniques		Privilege Escalation 13 techniques		Defense Evasion 40 techniques		Credential Access 15 techniques		Discovery 23 techniques		Lateral Movement 9 techniques		Collection 17 techniques	
Active Scanning (2)	Scanning IP Blocks	Domain	Drive-by Compromise	Virtual Private Server	Exploit Public-Facing Application	PowerShell	AppleScript	Account Manipulation (4)	Additional Cloud Credentials	Abuse Elevation Control Mechanism (4)	Setuid and Suidgid	Abuse Elevation Control Mechanism (4)	Bypass User Account Control	Adversary in-the-Middle (2)	LLMNR/NBTNS Poisoning and SMB Relay	Local Account	Exploitation of Remote Services	Adversary in-the-Middle (2)	LLMNR/NBTNS Poisoning and SMB Relay		
	Vulnerability Scanning		DNS Server																	Account Discovery (4)	Domain Account
Gather Victim Host Information (4)	Hardware	Acquire Infrastructure (8)	Server	External Remote Services	Command and Scripting Interpreter (9)	Windows Command Shell	Unix Shell	BITS Jobs	SSH Authorized Keys	Elevated Execution with Prompt	Token Impersonation/Theft	Create Process with Token	Access Token Manipulation (5)	Brute Force (4)	Password Guessing	Password Cracking	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Archive via Utility	
	Software		Virtual Private Server																		Server
Gather Victim Identity Information (2)	Firmware	Compromise Accounts (2)	Botnet	Web Services	Hardware Additions	Python	JavaScript	Network Device CLI	Registry Run Keys / Startup Folder	Token Impersonation/Theft	Create Process with Token	Make and Impersonate Token	Access Token Manipulation (5)	Parent PID Spoofing	Securityd Memory	Credentialed from Web Browsers	Remote Desktop Protocol	SSH Hijacking	Automated Collection		
	Client Configurations		Botnet																	Web Services	Hardware Additions
Gather Victim Network Information (8)	DNS	Compromise Infrastructure (8)	Domain Properties	DNS Server	Replication Through Removable Media	Container Administration Command	Deploy Container	Exploitation for Client Execution	Component Object Model	Dynamic Data Exchange	Boot or Logon Autostart Execution (13)	LSASS Driver	Shortcut Modification	Port Monitors	Print Processors	XDG Autostart Entries	Active Setup	Login Items	Systemd Timers	Container Orchestration Job	
	Network Trust Dependencies		Domain Properties																		DNS Server
Gather Victim Org Information (4)	Network Topology	Develop Capabilities (4)	Determine Physical Locations	Identify Business Tempo	Identify Roles	Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data	HWIDG	DNS/Passive DNS	Digital Certificates	CDNs	Scan Databases	Social Media	Search Engines	Search Victim-Owned Websites			
	Network Topology		Determine Physical Locations																Identify Business Tempo	Identify Roles	Spearphishing Service
Phishing for Information (2)	Identify Business Tempo	Establish Accounts (2)	Identify Roles	Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data	HWIDG	DNS/Passive DNS	Digital Certificates	CDNs	Scan Databases	Social Media	Search Engines	Search Victim-Owned Websites					
	Identify Business Tempo		Identify Roles														Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data
Search Closed Sources (2)	Identify Business Tempo	Obtain Capabilities (8)	Identify Roles	Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data	HWIDG	DNS/Passive DNS	Digital Certificates	CDNs	Scan Databases	Social Media	Search Engines	Search Victim-Owned Websites					
	Identify Business Tempo		Identify Roles														Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data
Search Open Technical Databases (3)	Identify Business Tempo	Stage Capabilities (8)	Identify Roles	Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data	HWIDG	DNS/Passive DNS	Digital Certificates	CDNs	Scan Databases	Social Media	Search Engines	Search Victim-Owned Websites					
	Identify Business Tempo		Identify Roles														Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data
Search Open Websites/Domains (2)	Identify Business Tempo	Stage Capabilities (8)	Identify Roles	Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data	HWIDG	DNS/Passive DNS	Digital Certificates	CDNs	Scan Databases	Social Media	Search Engines	Search Victim-Owned Websites					
	Identify Business Tempo		Identify Roles														Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data
Search Victim-Owned Websites	Identify Business Tempo	Stage Capabilities (8)	Identify Roles	Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data	HWIDG	DNS/Passive DNS	Digital Certificates	CDNs	Scan Databases	Social Media	Search Engines	Search Victim-Owned Websites					
	Identify Business Tempo		Identify Roles														Spearphishing Service	Spearphishing Attachment	Spearphishing Link	Threat Intel Vendors	Purchase Technical Data



## OS Credential Dumping

Sub-techniques (8)	
ID	Name
T1003.001	LSASS Memory
T1003.002	Security Account Manager
T1003.003	NTDS
T1003.004	LSA Secrets
T1003.005	Cached Domain Credentials
T1003.006	DCSync
T1003.007	Proc Filesystem
T1003.008	/etc/passwd and /etc/shadow

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](#) and access restricted information.

Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

ID: T1003
Sub-techniques: T1003.001, T1003.002, T1003.003, T1003.004, T1003.005, T1003.006, T1003.007, T1003.008
① Tactic: Credential Access
① Platforms: Linux, Windows, macOS
① Permissions Required: Administrator, SYSTEM, root
Contributors: Ed Williams, Trustwave, SpiderLabs; Vincent Le Toux
Version: 2.1
Created: 31 May 2017
Last Modified: 15 October 2021

[Version](#) [Permalink](#)

Unique endifier technique

Included Sub-techniques

Included Tactics

For which operating systems the attack is relevant

Rights required for the attack

The authors who described this attack

Version and TimeLine Detail

Included Technique

General describe about Technique

## Procedure Examples

ID	Name	Description
G0006	APT1	APT1 has been known to use credential dumping using Mimikatz. <sup>[5]</sup>
G0007	APT28	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims. <sup>[6][7]</sup> They have also dumped the LSASS process memory using the MiniDump function. <sup>[8]</sup>
G0022	APT3	APT3 has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig." <sup>[9]</sup>
G0050	APT32	APT32 used Mimikatz and customized versions of Windows Credential Dumper to harvest credentials. <sup>[10][11]</sup>
G0064	APT33	APT33 has used a variety of publicly available tools like LaZagne, Mimikatz, and ProcDump to dump credentials. <sup>[12][13]</sup>
G0087	APT39	APT39 has used Mimikatz, Windows Credential Editor and ProcDump to dump credentials. <sup>[14]</sup>

• Procedure Examples describes some cases relates with this Technique:

- Who used this Technique
- Some Details
- Links for sources

## Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing. <sup>[74]</sup>
M1043	Credential Access Protection	With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. It also does not protect against all forms of credential dumping. <sup>[75][76]</sup>
M1028	Operating System Configuration	Consider disabling or restricting NTLM. <sup>[77]</sup> Consider disabling WDigest authentication. <sup>[78]</sup>
M1027	Password Policies	Ensure that local administrator accounts have complex, unique passwords across all systems on the network.
M1026	Privileged Account Management	Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.

• Mitigations describes general advisees about how you can protect your environment



## References

1. Gruzweig, J. et al. (2021, March 2). Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities. Retrieved March 3, 2021.
2. Symantec. (2021, June 10). Attacks Against the Government Sector. Retrieved September 28, 2021.
3. Graeber, M. (2014, October). Analysis of Malicious Security Support Provider DLLs. Retrieved March 1, 2017.
4. Wilson, B. (2016, April 18). The Importance of KB2871997 and KB2928120 for Credential Protection. Retrieved April 11, 2018.
5. Mandiant. (n.d.). APT1 Exposing One of China's Cyber Espionage Units. Retrieved July 18, 2016.
6. ESET. (2016, October). En Route with Sednit - Part 2: Observing the Comings and Goings. Retrieved November 21, 2016.
7. Mueller, R. (2018, July 13). Indictment - United States of America vs. VIKTOR BORISOVICH NETYKSHQ, et al. Retrieved September 13, 2018.
8. NSA, CISA, FBI, NCSC. (2021, July). Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments. Retrieved July 26, 2021.
9. Symantec Security Response. (2016, September 6). Buckeye cyberespionage group shifts gaze from US to Hong Kong. Retrieved September 26, 2016.
10. Dahan, A. (2017, May 24). OPERATION COBALT KITTY: A LARGE-SCALE APT IN ASIA CARRIED OUT BY THE OCEANLOTUS GROUP. Retrieved November 5, 2018.
11. Dahan, A. (2017). Operation Cobalt Kitty. Retrieved December 27, 2018.
12. Security Response attack Investigation Team. (2019, March 27). Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S. Retrieved April 10, 2019.
13. Ackerman, G., et al. (2018, December 21). OVERRULED: Containing a Potentially Destructive Adversary. Retrieved January 17, 2019.
14. Hawley et al. (2019, January 29). APT39: An Iranian Cyber Espionage Group Focused on Personal Information. Retrieved February 19, 2019.
15. Fraser, N., et al. (2019, August 7). Double DragonAPT41, a dual espionage and cyber crime operation APT41. Retrieved September 23, 2019.
16. Rostovcev, N. (2021, June 10). Big airline heist APT41 likely behind a third-party attack on Air India. Retrieved August 26, 2021.
17. M.Léveillé, M-E.. (2017, October 24). Bad Rabbit: Not-Petya is back with improved ransomware. Retrieved January 28, 2021.
18. Lambert, T. (2020, May 7). Introducing Blue Mockingbird. Retrieved May 26, 2020.
19. Counter Threat Unit Research Team. (2017, October 12). BRONZE BUTLER Targets Japanese Enterprises. Retrieved January 4, 2018.
20. Cylance. (2014, December). Operation Cleaver. Retrieved September 14, 2017.
21. Strategic Cyber LLC. (2020, November 5). Cobalt Strike: Advanced Threat Tactics for Penetration Testers. Retrieved April 13, 2021.
22. F-Secure Labs. (2015, April 22). CozyDuke: Malware Analysis. Retrieved December 10, 2015.
23. DiMaggio, J. (2016, April 28). Tick cyberespionage group zeros in on Japan. Retrieved July 16, 2018.
24. Trend Micro. (2019, January 16). Exploring Emotet's Activities . Retrieved March 25, 2019.
25. Schroeder, W., Warner, J., Nelson, M. (n.d.). Github PowerShellEmpire. Retrieved April 28, 2016.
26. FireEye Threat Intelligence. (2016, April). Follow the Money: Dissecting the Operations of the Cyber Crime Group FIN6. Retrieved June 1, 2016.
27. McKeague, B. et al. (2019, April 5). Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware. Retrieved April 17, 2019.
28. Elovitz, S. & Ahl, I. (2016, August 18). Know Your Enemy: New Financially-Motivated & Spear-Phishing Group. Retrieved February 26, 2018.
42. Plan, F., et al. (2019, March 4). APT40: Examining a China-Nexus Espionage Actor. Retrieved March 18, 2019.
43. Mandiant. (2018). Mandiant M-Trends 2018. Retrieved July 9, 2018.
44. Deply, B. (n.d.). Mimikatz. Retrieved September 29, 2015.
45. Deply, B., Le Toux, V. (2016, June 5). module ~ Isadump. Retrieved August 7, 2017.
46. Grafnetter, M. (2015, October 26). Retrieving DPAPI Backup Keys from Active Directory. Retrieved December 19, 2017.
47. The Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NZ NCSC), CERT New Zealand, the UK National Cyber Security Centre (UK NCSC) and the US National Cybersecurity and Communications Integration Center (NCCIC). (2018, October 11). Joint report on publicly available hacking tools. Retrieved March 11, 2019.
48. Lancaster, T.. (2017, November 14). Muddying the Water: Targeted Attacks in the Middle East. Retrieved March 15, 2018.
49. Symantec DeepSight Adversary Intelligence Team. (2018, December 10). Seedworm: Group Compromises Government Agencies, Oil & Gas, NGOs, Telecoms, and IT Firms. Retrieved December 14, 2018.
50. Peretz, A. and Heck, E. (2021, March 5). Earth Vetala – MuddyWater Continues to Target Organizations in the Middle East. Retrieved March 18, 2021.
51. Chiu, A. (2016, June 27). New Ransomware Variant "Nyetya" Compromises Systems Worldwide. Retrieved March 26, 2019.
52. US-CERT. (2017, July 1). Alert (TA17-181A): Petya Ransomware. Retrieved March 15, 2019.
53. Unit 42. (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017.
54. Davis, S. and Caban, D. (2017, December 19). APT34 - New Targeted Attack in the Middle East. Retrieved December 20, 2017.
55. Bromiley, M., et al.. (2019, July 18). Hard Pass: Declining APT34's Invite to Join Their Professional Network. Retrieved August 26, 2019.
56. Hromcova, Z. (2019, July). OKRUM AND KETRICA: AN OVERVIEW OF RECENT KE3CHANG GROUP ACTIVITY. Retrieved May 6, 2020.
57. Mercer, W. and Rascagneres, P. (2018, February 12). Olympic Destroyer Takes Aim At Winter Olympics. Retrieved March 14, 2019.
58. Dantzig, M. v., Schamper, E. (2019, December 19). Operation Wocao: Shining a light on one of China's hidden hacking groups. Retrieved October 8, 2020.
59. Windows Defender Advanced Threat Hunting Team. (2016, April 29). PLATINUM: Targeted attacks in South and Southeast Asia. Retrieved February 15, 2018.
60. Mercer, W. et al. (2020, April 16). PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors. Retrieved April 27, 2020.
61. Nettitude. (2018, July 23). Python Server for PoshC2. Retrieved April 23, 2019.
62. PowerShellMafia. (2012, May 26). PowerSploit - A PowerShell Post-Exploitation Framework. Retrieved February 6, 2018.
63. PowerSploit. (n.d.). PowerSploit. Retrieved February 6, 2018.
64. Nicolas Verdier. (n.d.). Retrieved January 29, 2018.
65. CERT-FR. (2020, April 1). ATTACKS INVOLVING THE MESPINOZA/PYSA RANSOMWARE. Retrieved March 1, 2021.
66. Cherepanov, A.. (2016, December 13). The rise of TeleBots: Analyzing disruptive KillDisk attacks. Retrieved June 10, 2020.
67. Cherepanov, A.. (2017, June 30). TeleBots are back: Supply chain attacks against Ukraine. Retrieved June 11, 2020.
68. Group-IB. (2018, September). Silence: Moving Into the Darkside. Retrieved May 5, 2020.



# MITRE ATT&CK

14

Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Impact and Control 16 techniques	Exfiltration 9 techniques
Phishing Attachment	Command and Scripting Interpreter (A1)	Account Manipulation (A2) BITS Jobs (A2)	Abuse Elevation Control Mechanism (A4) Access Token Manipulation (A5)	Abuse Elevation Control Mechanism (A4) Access Token Manipulation (A5)	Adversary-in-the-Middle (A6) Brute Force (A7)	Account Discovery (A8) Application Window Discovery (A8) Browser Bookmark Discovery (A8) Cloud Infrastructure Discovery (A8) Cloud Service Dashboard (A8) Cloud Service Discovery (A8) Cloud Storage Object Discovery (A8) Container and Resource Discovery (A8) Domain Trust Discovery (A8) File and Directory Discovery (A8) Group Policy Discovery (A8) Network Service Scanning (A8) Network Share Discovery (A8) Network Sniffing (A8)	Exploitation of Remote Services (A9) Internal Spearphishing (A9) Lateral Tool Transfer (A9) Remote Service Session Hijacking (A9)	Adversary-in-the-Middle (A10) Archive Collected Data (A11) Archive via (A11) Audio Capture (A12) Automated Collection (A12) Browser Session Hijacking (A12) Clipboard Data (A12) Data from Cloud Storage Object (A12) Data from Configuration Repository (A12) Data from Information Repositories (A12) Data from Local System (A12) Data from Network Shared Drive (A12) Data from Removable Media (A12) Data Staged (A12) Email Collection (A12) Input Capture (A12) Screen Capture (A12) Video Capture (A12)	DNS (A13) File Transfer Protocols (A13) Mail Protocols (A13) Web Protocols (A13) DNS Calculation (A14) Domain Generation Algorithms (A14) Fast Flux DNS (A14) Encrypted Channel (A15) Fallback Channels (A15) Ingress Tool Transfer (A15) Multi-Stage Channels (A15) Non-Application Layer Protocol (A16) Non-Standard Port (A16) Protocol Tunneling (A16) Proxy (A16) Remote Access Software (A16) Traffic Signaling (A16) Web Service (A16)	Automated Exfiltration (A17) Data Transfer Size Limits (A17) Exfiltration Over Alternative Protocol (A18) Exfiltration Over C2 Channel (A18) Exfiltration Over Other Network Medium (A18) Exfiltration Over Physical Medium (A18) Exfiltration Over Web Service (A18) Scheduled Transfer (A18) Transfer Data to Cloud Account (A18)
Phishing Link	Container Administration Command (A19) Deploy Container (A19) Exploitation for Client Execution (A19) Inter-Process Communication (A19) Native API (A19)	Boot or Logon Autostart Execution (A20) Print Processors (A20) Re-opened Applications (A20) Registry Run Keys / Startup Folder (A20) Security Support Provider (A20) Shortcut Modification (A20) Time Providers (A20) Winlogon Helper DLL (A20) XDG Autostart Entries (A20)	Active Setup (A21) Authentication Package (A21) Kernel Modules and Extensions (A21) Login Items (A21) LSASS Driver (A21) Plist Modification (A21) Port Monitors (A21) Print Processors (A21) Re-opened Applications (A21) Registry Run Keys / Startup Folder (A21) Security Support Provider (A21) Shortcut Modification (A21) Time Providers (A21) Winlogon Helper DLL (A21) XDG Autostart Entries (A21)	Abuse Elevation Control Mechanism (A22) Access Token Manipulation (A22) Build Image on Host (A22) Deobfuscate/Decode Files or Information (A22) Deploy Container (A22) Direct Volume Access (A22) Domain Policy Modification (A22) Execution Guardrails (A22) Exploitation for Defense Evasion (A22) File and Directory Permissions Modification (A22) Hide Artifacts (A22) COR_PROFILER (A23) DLL Search Order Hijacking (A23) DLL Side-Loading (A23) Dylib Hijacking (A23) Dynamic Linker Hijacking (A23) Executable Installer File Permissions Weakness (A23) Path Interception by PATH Environment Variable (A23) Path Interception by Search Order Hijacking (A23) Path Interception by Unquoted Path (A23) Services File Permissions Weakness (A23) Services Registry Permissions Weakness (A23)	Credential Stuffing (A24) Password Cracking (A24) Password Guessing (A24) Password Spraying (A24) Credentialed API Hooking (A24) GUI Input Capture (A24) Keylogging (A24) Web Portal Capture (A24) Modify Authentication Process (A24) Network Sniffing (A24) /etc/passwd and /etc/shadow (A24) Cached Domain Credentials (A24) DCSync (A24) LSA Secrets (A24) LSASS Memory (A24) NTDS (A24) Proc Filesystem (A24) Security Account Manager (A24)	Account Discovery (A25) Application Window Discovery (A25) Browser Bookmark Discovery (A25) Cloud Infrastructure Discovery (A25) Cloud Service Dashboard (A25) Cloud Service Discovery (A25) Cloud Storage Object Discovery (A25) Container and Resource Discovery (A25) Domain Trust Discovery (A25) File and Directory Discovery (A25) Group Policy Discovery (A25) Network Service Scanning (A25) Network Share Discovery (A25) Network Sniffing (A25) Password Policy Discovery (A25) Peripheral Device Discovery (A25) Permission Groups Discovery (A25) Process Discovery (A25) Query Registry (A25) Remote System Discovery (A25) Software Discovery (A25) System Information Discovery (A25) System Location Discovery (A25) System Network Configuration Discovery (A25) System Network Connections Discovery (A25) System Owner/User Discovery (A25) System Service Discovery (A25) System Time (A25)	Distributed Component Object Model (A26) Remote Desktop Protocol (A26) SMB/Windows Admin Shares (A26) SSH (A26) VNC (A26) Windows Remote Management (A26)	Adversary-in-the-Middle (A27) Archive Collected Data (A28) Archive via (A28) Audio Capture (A29) Automated Collection (A29) Browser Session Hijacking (A29) Clipboard Data (A29) Data from Cloud Storage Object (A29) Data from Configuration Repository (A29) Data from Information Repositories (A29) Data from Local System (A29) Data from Network Shared Drive (A29) Data from Removable Media (A29) Data Staged (A29) Email Collection (A29) Input Capture (A29) Screen Capture (A29) Video Capture (A29)	DNS (A30) File Transfer Protocols (A30) Mail Protocols (A30) Web Protocols (A30) DNS Calculation (A31) Domain Generation Algorithms (A31) Fast Flux DNS (A31) Encrypted Channel (A32) Fallback Channels (A32) Ingress Tool Transfer (A32) Multi-Stage Channels (A32) Non-Application Layer Protocol (A33) Non-Standard Port (A33) Protocol Tunneling (A33) Proxy (A33) Remote Access Software (A33) Traffic Signaling (A33) Web Service (A33)	Automated Exfiltration (A34) Data Transfer Size Limits (A34) Exfiltration Over Alternative Protocol (A35) Exfiltration Over C2 Channel (A35) Exfiltration Over Other Network Medium (A35) Exfiltration Over Physical Medium (A35) Exfiltration Over Web Service (A35) Scheduled Transfer (A35) Transfer Data to Cloud Account (A35)
Phishing via Service	Container Administration Command (A36) Deploy Container (A36) Exploitation for Client Execution (A36) Inter-Process Communication (A36) Native API (A36)	Boot or Logon Autostart Execution (A37) Print Processors (A37) Re-opened Applications (A37) Registry Run Keys / Startup Folder (A37) Security Support Provider (A37) Shortcut Modification (A37) Time Providers (A37) Winlogon Helper DLL (A37) XDG Autostart Entries (A37)	Active Setup (A38) Authentication Package (A38) Kernel Modules and Extensions (A38) Login Items (A38) LSASS Driver (A38) Plist Modification (A38) Port Monitors (A38) Print Processors (A38) Re-opened Applications (A38) Registry Run Keys / Startup Folder (A38) Security Support Provider (A38) Shortcut Modification (A38) Time Providers (A38) Winlogon Helper DLL (A38) XDG Autostart Entries (A38)	Abuse Elevation Control Mechanism (A39) Access Token Manipulation (A39) Build Image on Host (A39) Deobfuscate/Decode Files or Information (A39) Deploy Container (A39) Direct Volume Access (A39) Domain Policy Modification (A39) Execution Guardrails (A39) Exploitation for Defense Evasion (A39) File and Directory Permissions Modification (A39) Hide Artifacts (A39) COR_PROFILER (A40) DLL Search Order Hijacking (A40) DLL Side-Loading (A40) Dylib Hijacking (A40) Dynamic Linker Hijacking (A40) Executable Installer File Permissions Weakness (A40) Path Interception by PATH Environment Variable (A40) Path Interception by Search Order Hijacking (A40) Path Interception by Unquoted Path (A40) Services File Permissions Weakness (A40) Services Registry Permissions Weakness (A40)	Credential Stuffing (A41) Password Cracking (A41) Password Guessing (A41) Password Spraying (A41) Credentialed API Hooking (A41) GUI Input Capture (A41) Keylogging (A41) Web Portal Capture (A41) Modify Authentication Process (A41) Network Sniffing (A41) /etc/passwd and /etc/shadow (A41) Cached Domain Credentials (A41) DCSync (A41) LSA Secrets (A41) LSASS Memory (A41) NTDS (A41) Proc Filesystem (A41) Security Account Manager (A41)	Account Discovery (A42) Application Window Discovery (A42) Browser Bookmark Discovery (A42) Cloud Infrastructure Discovery (A42) Cloud Service Dashboard (A42) Cloud Service Discovery (A42) Cloud Storage Object Discovery (A42) Container and Resource Discovery (A42) Domain Trust Discovery (A42) File and Directory Discovery (A42) Group Policy Discovery (A42) Network Service Scanning (A42) Network Share Discovery (A42) Network Sniffing (A42) Password Policy Discovery (A42) Peripheral Device Discovery (A42) Permission Groups Discovery (A42) Process Discovery (A42) Query Registry (A42) Remote System Discovery (A42) Software Discovery (A42) System Information Discovery (A42) System Location Discovery (A42) System Network Configuration Discovery (A42) System Network Connections Discovery (A42) System Owner/User Discovery (A42) System Service Discovery (A42) System Time (A42)	Distributed Component Object Model (A43) Remote Desktop Protocol (A43) SMB/Windows Admin Shares (A43) SSH (A43) VNC (A43) Windows Remote Management (A43)	Adversary-in-the-Middle (A44) Archive Collected Data (A45) Archive via (A45) Audio Capture (A46) Automated Collection (A46) Browser Session Hijacking (A46) Clipboard Data (A46) Data from Cloud Storage Object (A46) Data from Configuration Repository (A46) Data from Information Repositories (A46) Data from Local System (A46) Data from Network Shared Drive (A46) Data from Removable Media (A46) Data Staged (A46) Email Collection (A46) Input Capture (A46) Screen Capture (A46) Video Capture (A46)	DNS (A47) File Transfer Protocols (A47) Mail Protocols (A47) Web Protocols (A47) DNS Calculation (A48) Domain Generation Algorithms (A48) Fast Flux DNS (A48) Encrypted Channel (A49) Fallback Channels (A49) Ingress Tool Transfer (A49) Multi-Stage Channels (A49) Non-Application Layer Protocol (A50) Non-Standard Port (A50) Protocol Tunneling (A50) Proxy (A50) Remote Access Software (A50) Traffic Signaling (A50) Web Service (A50)	Automated Exfiltration (A51) Data Transfer Size Limits (A51) Exfiltration Over Alternative Protocol (A52) Exfiltration Over C2 Channel (A52) Exfiltration Over Other Network Medium (A52) Exfiltration Over Physical Medium (A52) Exfiltration Over Web Service (A52) Scheduled Transfer (A52) Transfer Data to Cloud Account (A52)
Phishing via Service	Container Administration Command (A53) Deploy Container (A53) Exploitation for Client Execution (A53) Inter-Process Communication (A53) Native API (A53)	Boot or Logon Autostart Execution (A54) Print Processors (A54) Re-opened Applications (A54) Registry Run Keys / Startup Folder (A54) Security Support Provider (A54) Shortcut Modification (A54) Time Providers (A54) Winlogon Helper DLL (A54) XDG Autostart Entries (A54)	Active Setup (A55) Authentication Package (A55) Kernel Modules and Extensions (A55) Login Items (A55) LSASS Driver (A55) Plist Modification (A55) Port Monitors (A55) Print Processors (A55) Re-opened Applications (A55) Registry Run Keys / Startup Folder (A55) Security Support Provider (A55) Shortcut Modification (A55) Time Providers (A55) Winlogon Helper DLL (A55) XDG Autostart Entries (A55)	Abuse Elevation Control Mechanism (A56) Access Token Manipulation (A56) Build Image on Host (A56) Deobfuscate/Decode Files or Information (A56) Deploy Container (A56) Direct Volume Access (A56) Domain Policy Modification (A56) Execution Guardrails (A56) Exploitation for Defense Evasion (A56) File and Directory Permissions Modification (A56) Hide Artifacts (A56) COR_PROFILER (A57) DLL Search Order Hijacking (A57) DLL Side-Loading (A57) Dylib Hijacking (A57) Dynamic Linker Hijacking (A57) Executable Installer File Permissions Weakness (A57) Path Interception by PATH Environment Variable (A57) Path Interception by Search Order Hijacking (A57) Path Interception by Unquoted Path (A57) Services File Permissions Weakness (A57) Services Registry Permissions Weakness (A57)	Credential Stuffing (A58) Password Cracking (A58) Password Guessing (A58) Password Spraying (A58) Credentialed API Hooking (A58) GUI Input Capture (A58) Keylogging (A58) Web Portal Capture (A58) Modify Authentication Process (A58) Network Sniffing (A58) /etc/passwd and /etc/shadow (A58) Cached Domain Credentials (A58) DCSync (A58) LSA Secrets (A58) LSASS Memory (A58) NTDS (A58) Proc Filesystem (A58) Security Account Manager (A58)	Account Discovery (A59) Application Window Discovery (A59) Browser Bookmark Discovery (A59) Cloud Infrastructure Discovery (A59) Cloud Service Dashboard (A59) Cloud Service Discovery (A59) Cloud Storage Object Discovery (A59) Container and Resource Discovery (A59) Domain Trust Discovery (A59) File and Directory Discovery (A59) Group Policy Discovery (A59) Network Service Scanning (A59) Network Share Discovery (A59) Network Sniffing (A59) Password Policy Discovery (A59) Peripheral Device Discovery (A59) Permission Groups Discovery (A59) Process Discovery (A59) Query Registry (A59) Remote System Discovery (A59) Software Discovery (A59) System Information Discovery (A59) System Location Discovery (A59) System Network Configuration Discovery (A59) System Network Connections Discovery (A59) System Owner/User Discovery (A59) System Service Discovery (A59) System Time (A59)	Distributed Component Object Model (A60) Remote Desktop Protocol (A60) SMB/Windows Admin Shares (A60) SSH (A60) VNC (A60) Windows Remote Management (A60)	Adversary-in-the-Middle (A61) Archive Collected Data (A62) Archive via (A62) Audio Capture (A63) Automated Collection (A63) Browser Session Hijacking (A63) Clipboard Data (A63) Data from Cloud Storage Object (A63) Data from Configuration Repository (A63) Data from Information Repositories (A63) Data from Local System (A63) Data from Network Shared Drive (A63) Data from Removable Media (A63) Data Staged (A63) Email Collection (A63) Input Capture (A63) Screen Capture (A63) Video Capture (A63)	DNS (A64) File Transfer Protocols (A64) Mail Protocols (A64) Web Protocols (A64) DNS Calculation (A65) Domain Generation Algorithms (A65) Fast Flux DNS (A65) Encrypted Channel (A66) Fallback Channels (A66) Ingress Tool Transfer (A66) Multi-Stage Channels (A66) Non-Application Layer Protocol (A67) Non-Standard Port (A67) Protocol Tunneling (A67) Proxy (A67) Remote Access Software (A67) Traffic Signaling (A67) Web Service (A67)	Automated Exfiltration (A68) Data Transfer Size Limits (A68) Exfiltration Over Alternative Protocol (A69) Exfiltration Over C2 Channel (A69) Exfiltration Over Other Network Medium (A69) Exfiltration Over Physical Medium (A69) Exfiltration Over Web Service (A69) Scheduled Transfer (A69) Transfer Data to Cloud Account (A69)
Phishing via Service	Container Administration Command (A70) Deploy Container (A70) Exploitation for Client Execution (A70) Inter-Process Communication (A70) Native API (A70)	Boot or Logon Autostart Execution (A71) Print Processors (A71) Re-opened Applications (A71) Registry Run Keys / Startup Folder (A71) Security Support Provider (A71) Shortcut Modification (A71) Time Providers (A71) Winlogon Helper DLL (A71) XDG Autostart Entries (A71)	Active Setup (A72) Authentication Package (A72) Kernel Modules and Extensions (A72) Login Items (A72) LSASS Driver (A72) Plist Modification (A72) Port Monitors (A72) Print Processors (A72) Re-opened Applications (A72) Registry Run Keys / Startup Folder (A72) Security Support Provider (A72) Shortcut Modification (A72) Time Providers (A72) Winlogon Helper DLL (A72) XDG Autostart Entries (A72)	Abuse Elevation Control Mechanism (A73) Access Token Manipulation (A73) Build Image on Host (A73) Deobfuscate/Decode Files or Information (A73) Deploy Container (A73) Direct Volume Access (A73) Domain Policy Modification (A73) Execution Guardrails (A73) Exploitation for Defense Evasion (A73) File and Directory Permissions Modification (A73) Hide Artifacts (A73) COR_PROFILER (A74) DLL Search Order Hijacking (A74) DLL Side-Loading (A74) Dylib Hijacking (A74) Dynamic Linker Hijacking (A74) Executable Installer File Permissions Weakness (A74) Path Interception by PATH Environment Variable (A74) Path Interception by Search Order Hijacking (A74) Path Interception by Unquoted Path (A74) Services File Permissions Weakness (A74) Services Registry Permissions Weakness (A74)	Credential Stuffing (A75) Password Cracking (A75) Password Guessing (A75) Password Spraying (A75) Credentialed API Hooking (A75) GUI Input Capture (A75) Keylogging (A75) Web Portal Capture (A75) Modify Authentication Process (A75) Network Sniffing (A75) /etc/passwd and /etc/shadow (A75) Cached Domain Credentials (A75) DCSync (A75) LSA Secrets (A75) LSASS Memory (A75) NTDS (A75) Proc Filesystem (A75) Security Account Manager (A75)	Account Discovery (A76) Application Window Discovery (A76) Browser Bookmark Discovery (A76) Cloud Infrastructure Discovery (A76) Cloud Service Dashboard (A76) Cloud Service Discovery (A76) Cloud Storage Object Discovery (A76) Container and Resource Discovery (A76) Domain Trust Discovery (A76) File and Directory Discovery (A76) Group Policy Discovery (A76) Network Service Scanning (A76) Network Share Discovery (A76) Network Sniffing (A76) Password Policy Discovery (A76) Peripheral Device Discovery (A76) Permission Groups Discovery (A76) Process Discovery (A76) Query Registry (A76) Remote System Discovery (A76) Software Discovery (A76) System Information Discovery (A76) System Location Discovery (A76) System Network Configuration Discovery (A76) System Network Connections Discovery (A76) System Owner/User Discovery (A76) System Service Discovery (A76) System Time (A76)	Distributed Component Object Model (A77) Remote Desktop Protocol (A77) SMB/Windows Admin Shares (A77) SSH (A77) VNC (A77) Windows Remote Management (A77)	Adversary-in-the-Middle (A78) Archive Collected Data (A79) Archive via (A79) Audio Capture (A80) Automated Collection (A80) Browser Session Hijacking (A80) Clipboard Data (A80) Data from Cloud Storage Object (A80) Data from Configuration Repository (A80) Data from Information Repositories (A80) Data from Local System (A80) Data from Network Shared Drive (A80) Data from Removable Media (A80) Data Staged (A80) Email Collection (A80) Input Capture (A80) Screen Capture (A80) Video Capture (A80)	DNS (A81) File Transfer Protocols (A81) Mail Protocols (A81) Web Protocols (A81) DNS Calculation (A82) Domain Generation Algorithms (A82) Fast Flux DNS (A82) Encrypted Channel (A83) Fallback Channels (A83) Ingress Tool Transfer (A83) Multi-Stage Channels (A83) Non-Application Layer Protocol (A84) Non-Standard Port (A84) Protocol Tunneling (A84) Proxy (A84) Remote Access Software (A84) Traffic Signaling (A84) Web Service (A84)	Automated Exfiltration (A85) Data Transfer Size Limits (A85) Exfiltration Over Alternative Protocol (A86) Exfiltration Over C2 Channel (A86) Exfiltration Over Other Network Medium (A86) Exfiltration Over Physical Medium (A86) Exfiltration Over Web Service (A86) Scheduled Transfer (A86) Transfer Data to Cloud Account (A86)
Phishing via Service	Container Administration Command (A87) Deploy Container (A87) Exploitation for Client Execution (A87) Inter-Process Communication (A87) Native API (A87)	Boot or Logon Autostart Execution (A88) Print Processors (A88) Re-opened Applications (A88) Registry Run Keys / Startup Folder (A88) Security Support Provider (A88) Shortcut Modification (A88) Time Providers (A88) Winlogon Helper DLL (A88) XDG Autostart Entries (A88)	Active Setup (A89) Authentication Package (A89) Kernel Modules and Extensions (A89) Login Items (A89) LSASS Driver (A89) Plist Modification (A89) Port Monitors (A89) Print Processors (A89) Re-opened Applications (A89) Registry Run Keys / Startup Folder (A89) Security Support Provider (A89) Shortcut Modification (A89) Time Providers (A89) Winlogon Helper DLL (A89) XDG Autostart Entries (A89)	Abuse Elevation Control Mechanism (A90) Access Token Manipulation (A90) Build Image on Host (A90) Deobfuscate/Decode Files or Information (A90) Deploy Container (A90) Direct Volume Access (A90) Domain Policy Modification (A90) Execution Guardrails (A90) Exploitation for Defense Evasion (A90) File and Directory Permissions Modification (A90) Hide Artifacts (A90) COR_PROFILER (A91) DLL Search Order Hijacking (A91) DLL Side-Loading (A91) Dylib Hijacking (A91) Dynamic Linker Hijacking (A91) Executable Installer File Permissions Weakness (A91) Path Interception by PATH Environment Variable (A91) Path Interception by Search Order Hijacking (A91) Path Interception by Unquoted Path (A91) Services File Permissions Weakness (A91) Services Registry Permissions Weakness (A91)	Credential Stuffing (A92) Password Cracking (A92) Password Guessing (A92) Password Spraying (A92) Credentialed API Hooking (A92) GUI Input Capture (A92) Keylogging (A92) Web Portal Capture (A92) Modify Authentication Process (A92) Network Sniffing (A92) /etc/passwd and /etc/shadow (A92) Cached Domain Credentials (A92) DCSync (A92) LSA Secrets (A92) LSASS Memory (A92) NTDS (A92) Proc Filesystem (A92) Security Account Manager (A92)	Account Discovery (A93) Application Window Discovery (A93) Browser Bookmark Discovery (A93) Cloud Infrastructure Discovery (A93) Cloud Service Dashboard (A93) Cloud Service Discovery (A93) Cloud Storage Object Discovery (A93) Container and Resource Discovery (A93) Domain Trust Discovery (A93) File and Directory Discovery (A93) Group Policy Discovery (A93) Network Service Scanning (A93) Network Share Discovery (A93) Network Sniffing (A93) Password Policy Discovery (A93) Peripheral Device Discovery (A93) Permission Groups Discovery (A93) Process Discovery (A93) Query Registry (A93) Remote System Discovery (A93) Software Discovery (A93) System Information Discovery (A93) System Location Discovery (A93) System Network Configuration Discovery (A93) System Network Connections Discovery (A93) System Owner/User Discovery (A93) System Service Discovery (A93) System Time (A93)	Distributed Component Object Model (A94) Remote Desktop Protocol (A94) SMB/Windows Admin Shares (A94) SSH (A94) VNC (A94) Windows Remote Management (A94)	Adversary-in-the-Middle (A95) Archive Collected Data (A96) Archive via (A96) Audio Capture (A97) Automated Collection (A97) Browser Session Hijacking (A97) Clipboard Data (A97) Data from Cloud Storage Object (A97) Data from Configuration Repository (A97) Data from Information Repositories (A97) Data from Local System (A97) Data from Network Shared Drive (A97) Data from Removable Media (A97) Data Staged (A97) Email Collection (A97) Input Capture (A97) Screen Capture (A97) Video Capture (A97)	DNS (A98) File Transfer Protocols (A98) Mail Protocols (A98) Web Protocols (A98) DNS Calculation (A99) Domain Generation Algorithms (A99) Fast Flux DNS (A99) Encrypted Channel (A100) Fallback Channels (A100) Ingress Tool Transfer (A100) Multi-Stage Channels (A100) Non-Application Layer Protocol (A101) Non-Standard Port (A101) Protocol Tunneling (A101) Proxy (A101) Remote Access Software (A101) Traffic Signaling (A101) Web Service (A101)	Automated Exfiltration (A102) Data Transfer Size Limits (A102) Exfiltration Over Alternative Protocol (A103) Exfiltration Over C2 Channel (A103) Exfiltration Over Other Network Medium (A103) Exfiltration Over Physical Medium (A103) Exfiltration Over Web Service (A103) Scheduled Transfer (A103) Transfer Data to Cloud Account (A103)
Phishing via Service	Container Administration Command (A104) Deploy Container (A104) Exploitation for Client Execution (A104) Inter-Process Communication (A104) Native API (A104)	Boot or Logon Autostart Execution (A105) Print Processors (A105) Re-opened Applications (A105) Registry Run Keys / Startup Folder (A105) Security Support Provider (A105) Shortcut Modification (A105) Time Providers (A105) Winlogon Helper DLL (A105) XDG Autostart Entries (A105)	Active Setup (A106) Authentication Package (A106) Kernel Modules and Extensions (A106) Login Items (A106) LSASS Driver (A106) Plist Modification (A106) Port Monitors (A106) Print Processors (A106) Re-opened Applications (A106) Registry Run Keys / Startup Folder (A106) Security Support Provider (A106) Shortcut Modification (A106) Time Providers (A106) Winlogon Helper DLL (A106) XDG Autostart Entries (A106)	Abuse Elevation Control Mechanism (A107) Access Token Manipulation (A107) Build Image on Host (A107) Deobfuscate/Decode Files or Information (A107) Deploy Container (A107) Direct Volume Access (A107) Domain Policy Modification (A107) Execution Guardrails (A107) Exploitation for Defense Evasion (A107) File and Directory Permissions Modification (A107) Hide Artifacts (A107) COR_PROFILER (A108) DLL Search Order Hijacking (A108) DLL Side-Loading (A108) Dylib Hijacking (A108) Dynamic Linker Hijacking (A108) Executable Installer File Permissions Weakness (A108) Path Interception by PATH Environment Variable (A108) Path Interception by Search Order Hijacking (A108) Path Interception by Unquoted Path (A108) Services File Permissions Weakness (A108) Services Registry Permissions Weakness (A108)	Credential Stuffing (A109) Password Cracking (A109) Password Guessing (A109) Password Spraying (A109) Credentialed API Hooking (A109) GUI Input Capture (A109) Keylogging (A109) Web Portal Capture (A109) Modify Authentication Process (A109) Network Sniffing (A109) /etc/passwd and /etc/shadow (A109) Cached Domain Credentials (A109) DCSync (A109) LSA Secrets (A109) LSASS Memory (A109) NTDS (A109) Proc Filesystem (A109) Security Account Manager (A109)	Account Discovery (A110) Application Window Discovery (A110) Browser Bookmark Discovery (A110) Cloud Infrastructure Discovery (A110) Cloud Service Dashboard (A110) Cloud Service Discovery (A110) Cloud Storage Object Discovery (A110) Container and Resource Discovery (A110) Domain Trust Discovery (A110) File and Directory Discovery (A110) Group Policy Discovery (A110) Network Service Scanning (A110) Network Share Discovery (A110) Network Sniffing (A110) Password Policy Discovery (A110) Peripheral Device Discovery (A110) Permission Groups Discovery (A110) Process Discovery (A110) Query Registry (A110) Remote System Discovery (A110) Software Discovery (A110) System Information Discovery (A110) System Location Discovery (A110) System Network Configuration Discovery (A110) System Network Connections Discovery (A110) System Owner/User Discovery (A110) System Service Discovery (A110) System Time (A110)	Distributed Component Object Model (A111) Remote Desktop Protocol (A111) SMB/Windows Admin Shares (A111) SSH (A111) VNC (A111) Windows Remote Management (A111)	Adversary-in-the-Middle (A112) Archive Collected Data (A113) Archive via (A113) Audio Capture (A114) Automated Collection (A114) Browser Session Hijacking (A114) Clipboard Data (A114) Data from Cloud Storage Object (A114) Data from Configuration Repository (A114) Data from Information Repositories (A114) Data from Local System (A114) Data from Network Shared Drive (A114) Data from Removable Media (A114) Data Staged (A114) Email Collection (A114) Input Capture (A114) Screen Capture (A114) Video Capture (A114)	DNS (A115) File Transfer Protocols (A115) Mail Protocols (A115) Web Protocols (A115) DNS Calculation (A116) Domain Generation Algorithms (A116) Fast Flux DNS (A116) Encrypted Channel (A117) Fallback Channels (A117) Ingress Tool Transfer (A117) Multi-Stage Channels (A117) Non-Application Layer Protocol (A118) Non-Standard Port (A118) Protocol Tunneling (A118) Proxy (A118) Remote Access Software (A118) Traffic Signaling (A118) Web Service (A118)	Automated Exfiltration (A119) Data Transfer Size Limits (A119) Exfiltration Over Alternative Protocol (A120) Exfiltration Over C2 Channel (A120) Exfiltration Over Other Network Medium (A120) Exfiltration Over Physical Medium (A120) Exfiltration Over Web Service (A120) Scheduled Transfer (A120) Transfer Data to Cloud Account (A120)
Phishing via Service	Container Administration Command (A121) Deploy Container (A121) Exploitation for Client Execution (A121) Inter-Process Communication (A121) Native API (A121)	Boot or Logon Autostart Execution (A122) Print Processors (A122) Re-opened Applications (A122) Registry Run Keys / Startup Folder (A122) Security Support Provider (A122) Shortcut Modification (A122) Time Providers (A122) Winlogon Helper DLL (A122) XDG Autostart Entries (A122)	Active Setup (A123) Authentication Package (A123) Kernel Modules and Extensions (A123) Login Items (A123) LSASS Driver (A123) Plist Modification (A123) Port Monitors (A123) Print Processors (A123) Re-opened Applications (A123) Registry Run Keys / Startup Folder (A123) Security Support Provider (A123) Shortcut Modification (A123) Time Providers (A123) Winlogon Helper DLL (A123) XDG Autostart Entries (A123)	Abuse Elevation Control Mechanism (A124) Access Token Manipulation (A124) Build Image on Host (A124) Deobfuscate/Decode Files or Information (A124) Deploy Container (A124) Direct Volume Access (A124) Domain Policy Modification (A124) Execution Guardrails (A124) Exploitation for Defense Evasion (A124) File and Directory Permissions Modification (A124) Hide Artifacts (A124) COR_PROFILER (A125) DLL Search Order Hijacking (A125) DLL Side-Loading (A125) Dylib Hijacking (A125) Dynamic Linker Hijacking (A125) Executable Installer File Permissions Weakness (A125) Path Interception by PATH Environment Variable (A125) Path Interception by Search Order Hijacking (A125) Path Interception by Unquoted Path (A125) Services File Permissions Weakness (A125) Services Registry Permissions Weakness (A125)	Credential Stuffing (A126) Password Cracking (A126) Password Guessing (A126) Password Spraying (A126) Credentialed API Hooking (A126) GUI Input Capture (A126) Keylogging (A126) Web Portal Capture (A126) Modify Authentication Process (A126) Network Sniffing (A126) /etc/passwd and /etc/shadow (A126) Cached Domain Credentials (A126) DCSync (A126) LSA Secrets (A126) LSASS Memory (A126) NTDS (A126) Proc Filesystem (A126) Security Account Manager (A126)	Account Discovery (A127) Application Window Discovery (A127) Browser Bookmark Discovery (A127) Cloud Infrastructure Discovery (A127) Cloud Service Dashboard (A127) Cloud Service Discovery (A127) Cloud Storage Object Discovery (A127) Container and Resource Discovery (A127) Domain Trust Discovery (A127) File and Directory Discovery (A127) Group Policy Discovery (A127) Network Service Scanning (A127) Network Share Discovery (A127) Network Sniffing (A127) Password Policy Discovery (A127) Peripheral Device Discovery (A127) Permission Groups Discovery (A127) Process Discovery (A127) Query Registry (A127) Remote System Discovery (A127) Software Discovery (A127) System Information Discovery (A127) System Location Discovery (A127) System Network Configuration Discovery (A127) System Network Connections Discovery (A127) System Owner/User Discovery (A127) System Service Discovery (A127) System Time (A127)	Distributed Component Object Model (A128) Remote Desktop Protocol (A128) SMB/Windows Admin Shares (A128) SSH (A128) VNC (A128) Windows Remote Management (A128)	Adversary-in-the-Middle (A129) Archive Collected Data (A130) Archive via (A130) Audio Capture (A131) Automated Collection (A131) Browser Session Hijacking (A131) Clipboard Data (A131) Data from Cloud Storage Object (A131) Data from Configuration Repository (A131) Data from Information Repositories (A131) Data from Local System (A131) Data from Network Shared Drive (A131) Data from Removable Media (A131) Data Staged (A131) Email Collection (A131) Input Capture (A131) Screen Capture (A131) Video Capture (A131)	DNS (A132) File Transfer Protocols (A132) Mail Protocols (A132) Web Protocols (A132) DNS Calculation (A	



- Who are we ?
- What APTs are attacking our sphere?
- What adversary's are dangerous for us?
- What does our environment consist of?
- What are our most valuable assets ?
- What protections do we have ?
- ...
- ...
- ...

Home > Groups > APT39

## APT39

APT39 is one of several names for cyberespionage activity conducted by the Iranian Ministry of Intelligence and Security (MOIS) through the front company Rana Intelligence Computing since at least 2014. APT39 has primarily targeted the travel, hospitality, academic, and telecommunications industries in Iran and across Asia, Africa, Europe, and North America to track individuals and entities considered to be a threat by the MOIS.<sup>[1][2][3][4][5]</sup>

ID: G0087

Associated Groups: REMIX KITTEN, ITG07, Chafer

Version: 3.1

Created: 19 February 2019

Last Modified: 12 October 2021

[Version Permalink](#)

### Associated Group Descriptions

Name	Description
REMIX KITTEN	[6]
ITG07	[3][4][5]
Chafer	Activities associated with APT39 largely align with a group publicly referred to as Chafer. <sup>[1][2][7][3][4][5]</sup>

### Techniques Used

ATT&CK Navigator Layers

Domain	ID	Name	Use
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	APT39 has used HTTP in communications with C2. <sup>[8][3]</sup>
		.004 Application Layer Protocol: DNS	APT39 has used remote access tools that leverage DNS in communications with C2. <sup>[8]</sup>
Enterprise	T1560	.001 Archive Collected Data: Archive via Utility	APT39 has used WinRAR and 7-Zip to compress an archive stolen data. <sup>[1]</sup>
Enterprise	T1197	BITS Jobs	APT39 has used the BITS protocol to exfiltrate stolen data from a compromised host. <sup>[3]</sup>
Enterprise	T1547	.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT39 has maintained persistence using the startup folder. <sup>[1]</sup>
		.009 Boot or Logon Autostart Execution: Shortcut Modification	APT39 has modified LNK shortcuts. <sup>[1]</sup>

• General describe about actor and it activity in the world

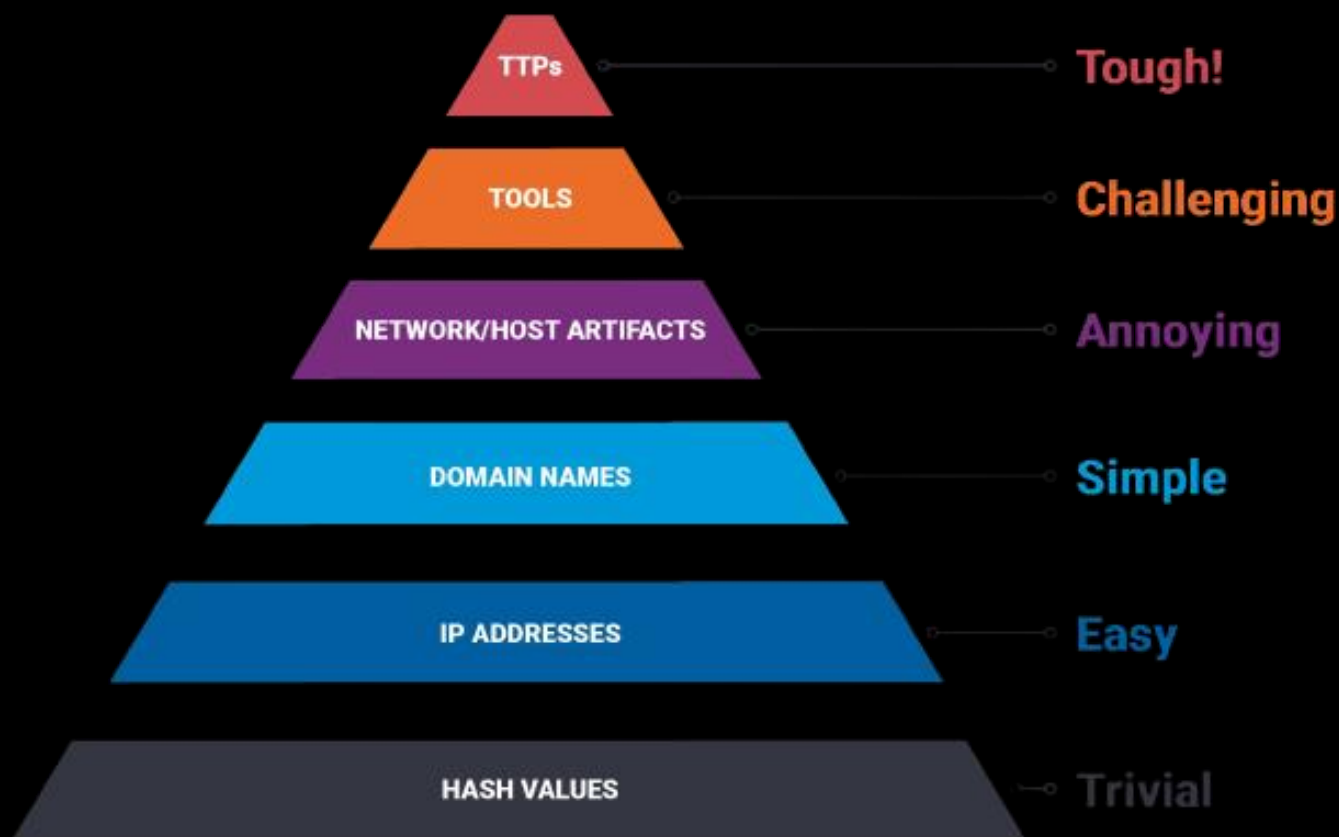
• Related alias

• Which TTPs they used in detected activity

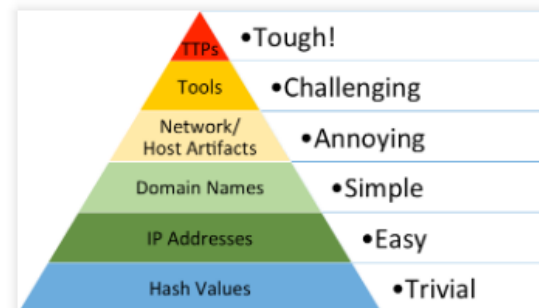


# The Pyramid of Pain

17



## The Pyramid of Pain



To illustrate this concept, I have created what I like to call the Pyramid of Pain. This simple diagram shows the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them. Let's examine this diagram in more detail.

### Types of Indicators

Let's start by simply defining types of indicators make up the pyramid:

1. **Hash Values:** SHA1, MD5 or other similar hashes that correspond to specific suspicious or malicious files. Often used to provide unique references to specific samples of malware or to files involved in an intrusion.
2. **IP Addresses:** It's, um, an IP address. Or maybe a netblock.
3. **Domain Names:** This could be either a domain name itself (e.g., "evil.net") or maybe even a sub- or sub-sub-domain (e.g., "this.is.sooooo.evil.net")
4. **Network Artifacts:** Observables caused by adversary activities on your network. Technically speaking, every byte that flows over your network as a result of the adversary's interaction could be an artifact, but in practice this really means those pieces of the activity that might tend to distinguish malicious activity from that of legitimate users. Typical examples might be URI patterns, C2 information embedded in network protocols, distinctive HTTP User-Agent or SMTP Mailer values, etc.
5. **Host Artifacts:** Observables caused by adversary activities on one or more of your hosts. Again, we focus on things that would tend to distinguish malicious activities from legitimate ones. They could be registry keys or values known to be created by specific pieces of malware, files or directories dropped in certain places or using certain names, names or descriptions or malicious services or almost anything else that's distinctive.
6. **Tools:** Software used by the adversary to accomplish their mission. Mostly this will be things they bring with them, rather than software or commands that may already be installed on the computer. This would include utilities designed to create malicious documents for spearphishing, backdoors used to establish C2 or password crackers or other host-based utilities they may want to use post-compromise.
7. **Tactics, Techniques and Procedures (TTPs):** How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between. "Spearphishing" is a common TTP for establishing a presence in the network. "Spearphishing with a trojaned PDF file" or "... with a link to a malicious .SCR file disguised as a ZIP" would be more specific versions. "Dumping cached authentication credentials and reusing them in Pass-the-Hash attacks" would be a TTP. Notice we're not talking about specific tools here, as there are a number of ways of weaponizing a PDF or implementing Pass-the-Hash.

# MITRE ATT&CK

18

Initial Access 9 techniques		Execution 12 techniques		Persistence 19 techniques		Privilege Escalation 13 techniques		Defense Evasion 40 techniques		Credential Access 15 techniques		Discovery 29 techniques		Lateral Movement 9 techniques		Collection 17 techniques																																																																																																																				
Drive-by Compromise	Exploit Public-Facing Application	External Remote Services	Hardware Additions	Spearphishing Attachment	Spearphishing Link	Spearphishing via Service	Container Administration Command	Boot or Logon Autostart Execution (2/19)	Deploy Container	Exploitation for Client Execution	Inter-Process Communication (2/2)	Native API	At (Linux)	At (Windows)	Container Orchestration Job	Cron	Scheduled Task	Systemd Timers	Shared Modules	Software Deployment Tools	System Services (1/2)	Service Execution	Malicious File	User Execution (2/3)	Malicious Image	Malicious Link	Windows Management Instrumentation	Account Manipulation (2/4)	BITS Jobs	Active Setup	Authentication Package	Kernel Modules and Extensions	Login Items	LSASS Driver	Plist Modification	Port Monitors	Print Processors	Re-opened Applications	Registry Run Keys / Startup Folder	Security Support Provider	Shortcut Modification	Time Providers	Winlogon Helper DLL	XDG Autostart Entries	Abuse Elevation Control Mechanism (2/4)	Access Token Manipulation (2/6)	Active Setup	Authentication Package	Kernel Modules and Extensions	Login Items	LSASS Driver	Plist Modification	Port Monitors	Print Processors	Re-opened Applications	Registry Run Keys / Startup Folder	Security Support Provider	Shortcut Modification	Time Providers	Winlogon Helper DLL	XDG Autostart Entries	Abuse Elevation Control Mechanism (2/4)	Access Token Manipulation (2/6)	Build Image on Host	Deobfuscate/Decode Files or Information	Deploy Container	Direct Volume Access	Domain Policy Modification (2/2)	Execution Guardrails (2/7)	Exploitation for Defense Evasion	File and Directory Permissions Modification (2/2)	Hide Artifacts	Hijack Execution Flow (2/11)	Impair Defenses (2/9)	Adversary-in-the-Middle (2/2)	Brute Force (2/4)	Credentials from Password Stores	Exploitation for Credential Access	Forced Authentication	Forge Web Credentials (2/2)	Account Discovery (2/4)	Application Window Discovery	Browser Bookmark Discovery	Cloud Infrastructure Discovery	Cloud Service Dashboard	Cloud Service Discovery	Cloud Storage Object Discovery	Container and Resource Discovery	Domain Trust Discovery	File and Directory Discovery	Group Policy Discovery	Network Service Scanning	Network Share Discovery	Network Sniffing	Password Policy Discovery	Peripheral Device Discovery	Permission Groups Discovery (2/8)	Process Discovery	Query Registry	Remote System Discovery	Software Discovery	System Location Discovery (2/7)	System Network Configuration Discovery (2/1)	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	System Time Discovery	Virtualization Evasion (2/7)	Sandbox	Adversary-in-the-Middle (2/2)	Archive Collected Data (1/4)	Archive via Custom Method	Archive via Library	Archive via Utility	Audio Capture	Automated Collection	Browser Session Hijacking	Distributed Component Object Model	Remote Desktop Protocol	Clipboard Data	Data from Cloud Storage Object	SSH	VNC	Data from Configuration Repository (2/2)	Data from Information Repositories (2/3)	Data from Local	Local Data Staging	Remote Data Staging	Credential API Hooking	GUI Input Capture	Keylogging	Portal Capture
Exploit Public-Facing Application							JavaScript		Account Manipulation (2/4)	Abuse Elevation Control Mechanism (2/4)	Abuse Elevation Control Mechanism (2/4)	Adversary-in-the-Middle (2/2)	Account Discovery (2/4)	Exploitation of Remote Services	Internal Spearphishing	Archive Collected Data (1/4)	Archive via Custom Method	Audio Capture	Automated Collection	Browser Session Hijacking	Distributed Component Object Model	Remote Desktop Protocol	Clipboard Data	Data from Cloud Storage Object	SSH	VNC	Data from Configuration Repository (2/2)	Data from Information Repositories (2/3)	Data from Local	Local Data Staging	Remote Data Staging	Credential API Hooking	GUI Input Capture	Keylogging	Portal Capture																																																																																																	
External Remote Services							PowerShell		Account Manipulation (2/4)	Abuse Elevation Control Mechanism (2/4)	Abuse Elevation Control Mechanism (2/4)	Adversary-in-the-Middle (2/2)	Account Discovery (2/4)	Exploitation of Remote Services	Internal Spearphishing	Archive Collected Data (1/4)	Archive via Custom Method	Audio Capture	Automated Collection	Browser Session Hijacking	Distributed Component Object Model	Remote Desktop Protocol	Clipboard Data	Data from Cloud Storage Object	SSH	VNC	Data from Configuration Repository (2/2)	Data from Information Repositories (2/3)	Data from Local	Local Data Staging	Remote Data Staging	Credential API Hooking	GUI Input Capture	Keylogging	Portal Capture																																																																																																	
Hardware Additions							Python		Account Manipulation (2/4)	Abuse Elevation Control Mechanism (2/4)	Abuse Elevation Control Mechanism (2/4)	Adversary-in-the-Middle (2/2)	Account Discovery (2/4)	Exploitation of Remote Services	Internal Spearphishing	Archive Collected Data (1/4)	Archive via Custom Method	Audio Capture	Automated Collection	Browser Session Hijacking	Distributed Component Object Model	Remote Desktop Protocol	Clipboard Data	Data from Cloud Storage Object	SSH	VNC	Data from Configuration Repository (2/2)	Data from Information Repositories (2/3)	Data from Local	Local Data Staging	Remote Data Staging	Credential API Hooking	GUI Input Capture	Keylogging	Portal Capture																																																																																																	
Phishing (2/3)	Spearphishing Link	Spearphishing via Service	Container Administration Command	Boot or Logon Autostart Execution (2/19)	Deploy Container	Exploitation for Client Execution	Inter-Process Communication (2/2)	Native API	At (Linux)	At (Windows)	Container Orchestration Job	Cron	Scheduled Task	Systemd Timers	Shared Modules	Software Deployment Tools	System Services (1/2)	Service Execution	Malicious File	User Execution (2/3)	Malicious Image	Malicious Link	Windows Management Instrumentation	Account Manipulation (2/4)	BITS Jobs	Active Setup	Authentication Package	Kernel Modules and Extensions	Login Items	LSASS Driver	Plist Modification	Port Monitors	Print Processors	Re-opened Applications	Registry Run Keys / Startup Folder	Security Support Provider	Shortcut Modification	Time Providers	Winlogon Helper DLL	XDG Autostart Entries	Abuse Elevation Control Mechanism (2/4)	Access Token Manipulation (2/6)	Active Setup	Authentication Package	Kernel Modules and Extensions	Login Items	LSASS Driver	Plist Modification	Port Monitors	Print Processors	Re-opened Applications	Registry Run Keys / Startup Folder	Security Support Provider	Shortcut Modification	Time Providers	Winlogon Helper DLL	XDG Autostart Entries	Abuse Elevation Control Mechanism (2/4)	Access Token Manipulation (2/6)	Build Image on Host	Deobfuscate/Decode Files or Information	Deploy Container	Direct Volume Access	Domain Policy Modification (2/2)	Execution Guardrails (2/7)	Exploitation for Defense Evasion	File and Directory Permissions Modification (2/2)	Hide Artifacts	Hijack Execution Flow (2/11)	Impair Defenses (2/9)	Adversary-in-the-Middle (2/2)	Brute Force (2/4)	Credentials from Password Stores	Exploitation for Credential Access	Forced Authentication	Forge Web Credentials (2/2)	Account Discovery (2/4)	Application Window Discovery	Browser Bookmark Discovery	Cloud Infrastructure Discovery	Cloud Service Dashboard	Cloud Service Discovery	Cloud Storage Object Discovery	Container and Resource Discovery	Domain Trust Discovery	File and Directory Discovery	Group Policy Discovery	Network Service Scanning	Network Share Discovery	Network Sniffing	Password Policy Discovery	Peripheral Device Discovery	Permission Groups Discovery (2/8)	Process Discovery	Query Registry	Remote System Discovery	Software Discovery	System Location Discovery (2/7)	System Network Configuration Discovery (2/1)	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	System Time Discovery	Virtualization Evasion (2/7)	Sandbox	Adversary-in-the-Middle (2/2)	Archive Collected Data (1/4)	Archive via Custom Method	Archive via Library	Archive via Utility	Audio Capture	Automated Collection	Browser Session Hijacking	Distributed Component Object Model	Remote Desktop Protocol	Clipboard Data	Data from Cloud Storage Object	SSH														

## Other Sources for Global Threat Analysis

19



# Common TTPs of modern ransomware groups





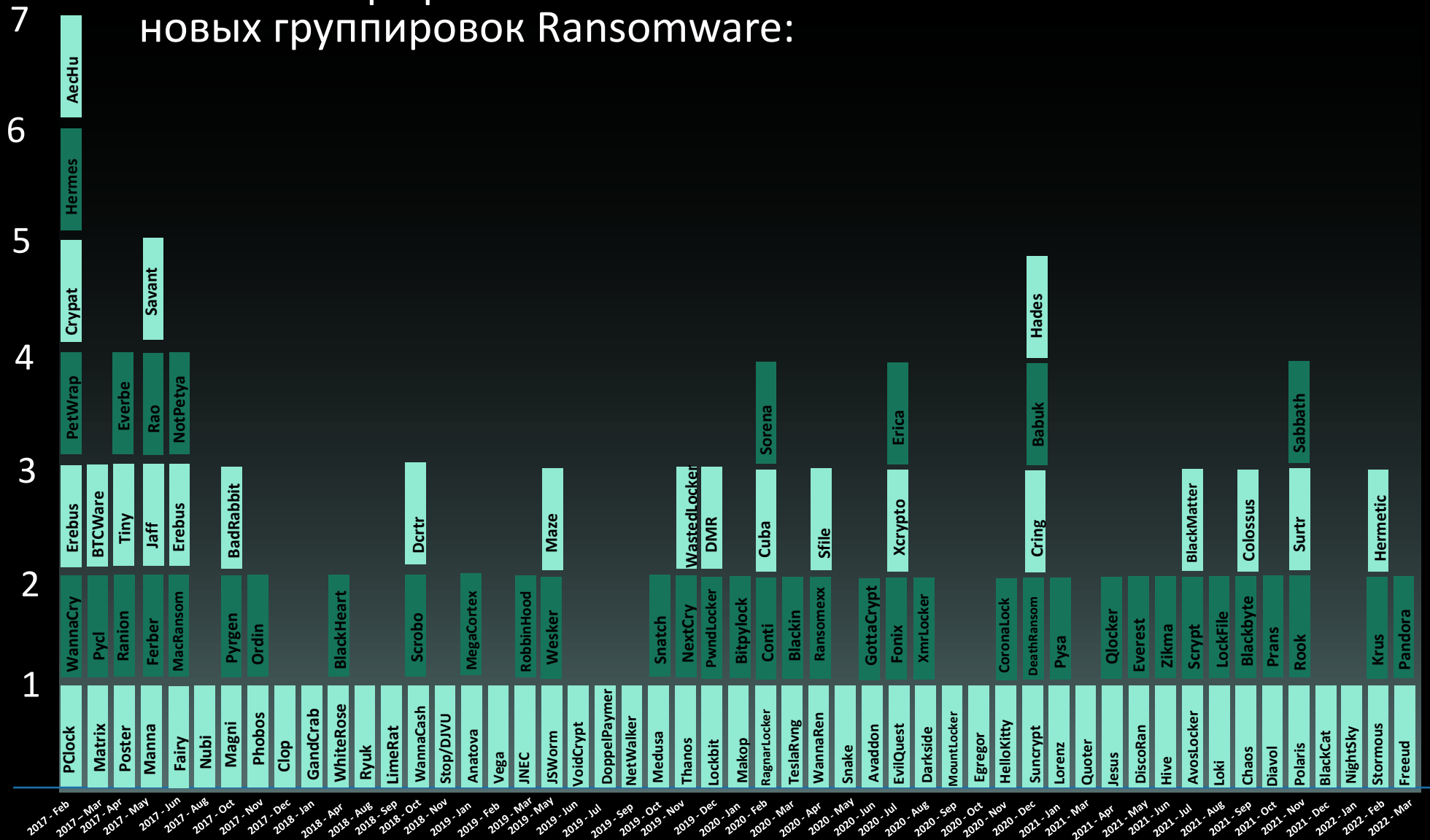
“Intelligence – is the glue that can bind together multiple diverse teams operating at different levels with different priorities”

---

“Intelligence Driven Incident Response” by Scott J. Roberts & Rebekah Brown



На основе нашей статистики мы составили график появления новых группировок Ransomware:



---

Мы выбрали восемь наиболее активных групп Ransomware, а именно:

1 <b>Conti/Ryuk</b>	2 <b>Pysa</b>	3 <b>Clop (TA505)</b>	4 <b>Hive</b>
5 <b>Lockbit2.0</b>	6 <b>RagnarLocker</b>	7 <b>BlackByte</b>	8 <b>BlackCat</b>



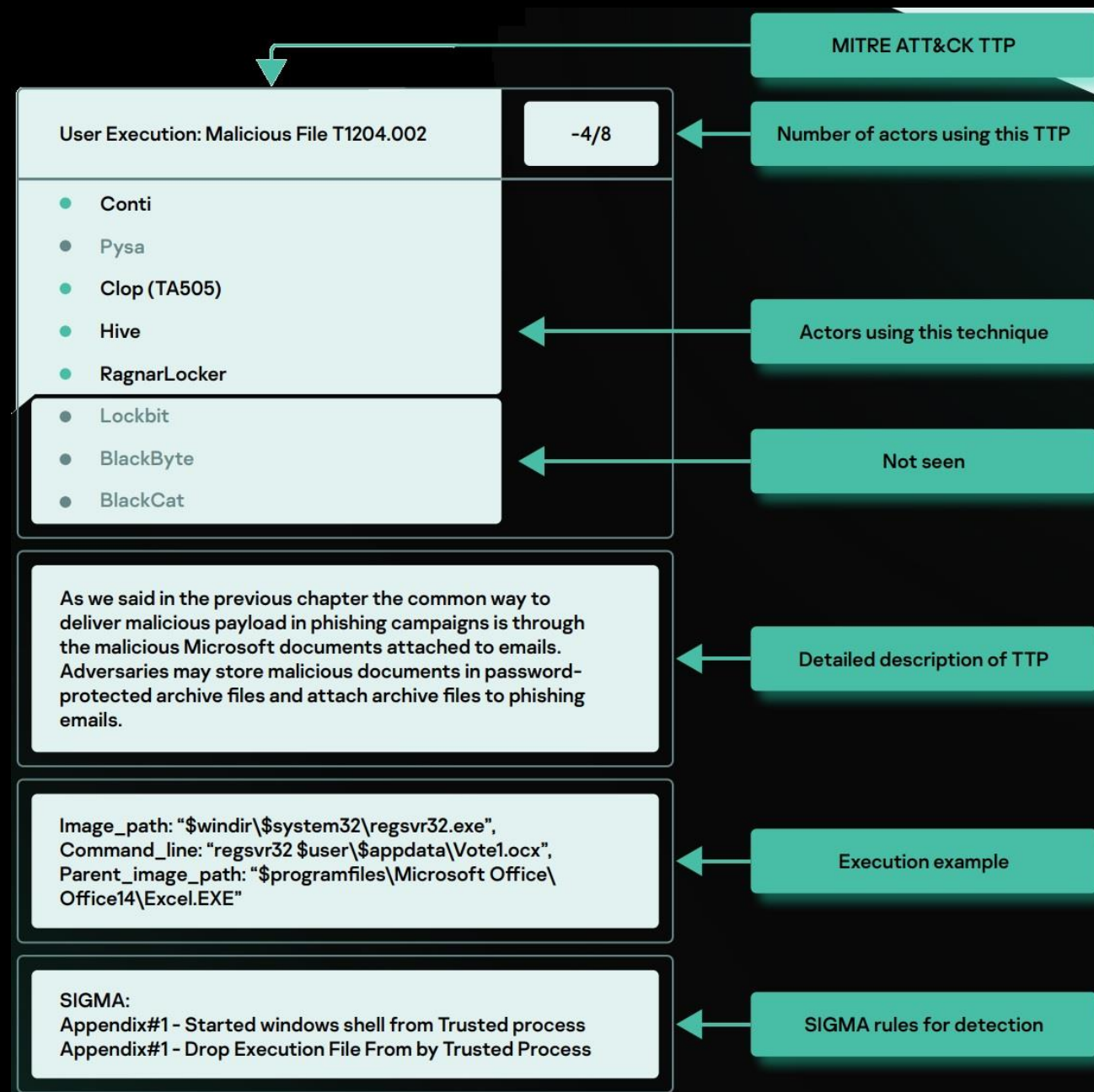
# Cyber Kill Chain

Чтобы выделить общие паттерны различных схем атак и TTPs, используемые различными группами вымогателей, мы создали диаграмму Cyber Kill Chain.



# Technical Details

Каждая из техник, показанная на предыдущей диаграмме, сопоставлена с группами и сопровождается таблицей, показывающей, кто из обсуждаемых группировок использовал данную технику.



# Common TTPs

Initial Access	External Remote Services T1133	Exploit Public Facing Application T1190	Phishing T1566						
Execution	User Execution: Malicious File T1204.002	Command and Scripting Interpreter T1059	Windows Management Instrumentation T1047						
Persistence	Scheduled Task T1053.005	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	Account Manipulation T1098	Create or Modify System Process: Windows Service T1543.003	BITS Jobs T1197				
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002	Exploitation for Privilege Escalation T1068	Access Token Manipulation T1134						
Defense Evasion	Signed Binary Proxy Execution T1218	Process Injection T1055	Impair Defenses: Disable or Modify System Firewall T1562.004	Impair Defenses: Disable or Modify Tools T1562.001	Masquerading T1036	Indicator Removal on Host: File Deletion T1070.004	Indicator Removal on Host: Clear Windows Event Logs T1070.001	Deobfuscate/ Decode Files or Information T1140	
Credential Access	OS Credential Dumping: LSASS Memory T1003.001	Credentials from Password Stores: Credentials from Web Browsers T1555.003	Brute Force T1110						
Discovery	System Network Connections Discovery T1049	Remote System Discovery T1018	Network Share Discovery T1135	Account Discovery T1087	File and Directory Discovery T1083	Process Discovery T1057			
Lateral Movement	Remote Services: Remote Desktop Protocol T1021.001	Lateral Tool Transfer T1570	Remote Services: SMB/ Windows Admin Shares T1021.002						
Command and Control	Application Layer Protocol: Web Protocols T1071.001								
Exfiltration	Exfiltration Over C2 Channel T1041	Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002							
Impact	Inhibit System Recovery T1490	Service Stop T1489							

# Mitigations

Мы собрали лучшие практики из NIST, NCSC, CISA, SANS в организованную структуру, которую можно применять в организациях.

We highlight the following stages of a ransomware incident, that can be mitigated or hampered for adversaries by defenders:

28

## Intrusion

At the intrusion stage, an adversary tries to break into a protected perimeter  
Examples: spear phishing emails, bruteforce internet-facing services (RDP)

- ➔ **The Defenders' Main Goal:**  
Prevent the malware from reaching the devices

## Exploitation

At the exploitation stage, an adversary tries to run code in order to escalate privileges, access and exfiltrate sensitive information, or harvest credentials

- ➔ **The Defenders' Main Goal:**  
Prevent malware from launching on endpoint devices

## Lateral Movement

At the lateral movement stage, an adversary tries to spread across the network

- ➔ **The Defenders' Main Goal:**  
Prevent malware from reaching other devices

There are additional measures that can be taken to make your organization more secure: Countering data loss and Preparing for an incident



# Victims

Для этого анализа мы использовали статистические источники по обнаружениям, а также источники объявлений в даркнете о жертвах, размещенных операторами Ransomware.



# Sigma Rules

Также мы создали SIGMA правила которые вы можете использовать в своих SIEM системах чтобы обнаруживать активность противника в собственной инфраструктуре.

Techniques	SIGMA
Exploit Public-Facing Application T1190	<ul style="list-style-type: none"><li>Windows Shell Start by Web Applications</li></ul>
User Execution T1204	<ul style="list-style-type: none"><li>Started windows shell from Trusted process</li><li>Drop Execution File From by Trusted Process</li></ul>
Command and Scripting Interpreter T1059	Available in the full version of the report in Kaspersky TIP: <ul style="list-style-type: none"><li>Execution of Downloaded Powershell Code</li><li>Encoded/decoded PowerShell Code Execution</li><li>Executing PS1 from Public Directory</li><li>Powershell Suspicious Arguments</li><li>Executing JavaScript from Public Directories</li></ul>
Windows Management Instrumentation T1047	Available in the full version of the report in Kaspersky TIP: <ul style="list-style-type: none"><li>Suspicious Command wmic.exe</li><li>Suspicious Child Process Wmiprvse.exe</li></ul>
Scheduled Task/Job: Scheduled Task T1053.005	<ul style="list-style-type: none"><li>Scheduled Task Start from Public Directory</li><li>Windows Shell Started Schtasks</li></ul>
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	Available in the full version of the report in Kaspersky TIP: <ul style="list-style-type: none"><li>Modification Main Registry Run Keys</li><li>Adding Path of Open Folder in Run Keys via Registry</li><li>Adding Suspicious File in Autorun Keys via Registry</li><li>Suspicious File Creation in Startup Folder</li></ul>
Account Manipulation T1098	Available in the full version of the report in Kaspersky TIP: <ul style="list-style-type: none"><li>Account Creation via Powershell</li><li>Account Creation via net.exe</li><li>Adding Account in Domain or Local Admin Group via net.exe</li><li>Adding Account in Domain or Local Admin Group via PowerShell</li></ul>
Create or Modify System Process: Windows Service T1543.003	Available in the full version of the report in Kaspersky TIP: <ul style="list-style-type: none"><li>Service Installation From Non-System Directory</li><li>Service Image Path Modification via sc.exe</li></ul>
BITS Jobs T1197	Available in the full version of the report in Kaspersky TIP: <ul style="list-style-type: none"><li>File Download via Bitsadmin</li><li>Suspicious Jobs via Bitsadmin</li></ul>
Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002	<ul style="list-style-type: none"><li>UAC Bypass via COM Object</li><li>Disabling UAC via Registry</li></ul>

## No More Ransom! Don't!

31



“ Иногда есть возможность помочь пользователю, зараженному Ransomware, вернуть доступ к зашифрованным данным без уплаты выкупа.

Мы создали коллекцию ключей и утилит, которые могут помочь пользователям восстановить доступ к своим системам, атакованным Ransomware группировками.

Report



Vote



Thank you!

kaspersky